Truly Random Number Generator Promises Stronger Encryption Across All Devices, Cloud

March 4, 2016

SAN FRANCISCO, RSA Conference -- In light of yet another SSL vulnerability this week, any improvements to the underpinnings of encryption would be welcome. One weakness of encryption algorithms -- one that simply increasing from 128-bit to 256-bit can't solve -- is that they are based on *pseudo*-random number generators; not *truly* random number generators.

Whitewood Encryption Systems, which launched in summer 2015, is changing that, by using quantum mechanics.

They generate truly random numbers by harnessing the entropy (randomness or disorder) of nature, which is much more random than any of the sources computing systems currently glean for entropy.

Two problems with old entropy collection

Entropy is collected at the hardware level, typically by actions like keystrokes and mouse movements. There are two troubles here.

One: keystrokes and mouse movements don't create enough entropy.

In a Linux kernel, the entropy is used to create random characters that are put in two special files: dev/random and dev/urandom. As Richard Moulds, Whitewood's vice-president of business development and strategy, describes it, dev/random is the good drinking water -- the true random numbers -- while dev/urandom may be fine for industrial uses, but you wouldn't want to drink it. If the two were faucets, the usual amount of entropy would produce a steady flow of dev/urandom, but only a few drips of the delicious dev/random. So, when an application -- even a cryptographic application -- calls for a random number, they might get one of those low-quality urandom ones.

Two: Since entropy is generated from hardware, every layer of abstraction from the hardware will have reduced access to entropy -- and that's troubling for anyone who uses virtualization.

"One bad reason to do virtualization," says Moulds, "is it's a firewall for entropy. In the virtual world, there ain't no randomness."

Sharing randomness

The product Whitewood launched with in August, the Entropy Engine, addresses the first problem. It turns the drip of drinking water into a steady flow.

The natural world has light and sound to draw entropy from, but certain environments aren't particularly changeable -- a datacenter, for example, is usually just full of white noise and immobile machinery -- so it's not a great source of randomness. So, what Whitewood does is

put a quantum optical field right inside the server, and capture the randomness of the photons' naturally unpredictable behavior. (Photons are naturally prone to bunching up, unbunching, then bunching up again, causing the optical field to dim, brighten, and flicker in a completely random way.)

One of the products Whitewood launched at RSA this week, NetRandom, addresses the second problem.

As Raymond Newell, research scientist at Los Alamos National Laboratory and contributor to Whitewood's creation, explains, "We take the randomness we create and spread it across the network."

Before, Entropy Engine only worked on the local device. With NetRandom, they can feed randomness through the network and strengthen the encryption used by virtual machines, cloud instances, clients, servers, and embedded systems in Internet of Things devices. "One of them could support tens of thousands of virtual machines," says Newell.

Any application that uses cryptography can benefit, without needing to make any modifications; and without needing any help from their cloud service providers or IoT device manufacturers.

Newell believes this will be a boon for security on industrial control systems' and other embedded systems that are expected to last 10 to 20 years with minimal support. "One of the reasons we like quantum mechanics is because we're confident it's going to keep up," he says.

Whitewood also announced a partnership with wolfSSL, a company that sells stripped-down crypto toolkits for embedded systems that don't run full-blown operating systems -- like ATMs and IoT devices. The partnership will allow wolfSSL to provide that stronger encryption to customers.

Whitewood also announced an integration with Cryptsoft, an OEM provider of a key management integration protocol. The integration, says Newell, "allows to attest to the origin of the keys," which improves key management and can could further empower digital signatures.

This article originally appeared in Dark Reading Information Week.

RICHARD P. FEYNMAN CENTER FOR INNOVATION

www.lanl.gov/feynmancenter | (505) 667-9090 | feynmancenter@lanl.gov